VETUMA
Electronic identification and signature service for citizens

Uses Cases: Identification, Signature

Brussels 23th April 2007
Mira Nivala, State IT Management Unit
Ministry of Finance, Finland
mira.nivala@vm.fi
VETUMA-service: Electronic identification, signature and payment service for citizens

- **Applicat**on
  - Authenticate
  - Sign
  - Pay
  - Adaptation

- **VETUMA**
  - Smart card (qualified certificates)
  - Password
  - e-banks
  - Mobile phone (qualified certificates)
  - New methods (e.g., Biometric, such as palm vein)

- Authentication methods with different programming interfaces
- Network payment services with different programming interfaces
- Electronic signature devices with different programming interfaces
- New e-payment methods

**VETUMA-service**: Electronic identification, signature and payment service for citizens

**MINISTRY OF FINANCE**
Mira Nivala, State IT Management Unit

24.4.2007
Use Case: Flow of the VETUMA identification

1. User wants to fill in an application which requires identification

2. Service application
   • ensures that connection uses SSL/TSL
   • creates the request for VETUMA
   • forwards the request through the user's browser to the VETUMA-service

3. VETUMA-service
   • ensures validity of the request
   • if ok, opens the VETUMA User Interface to the user's browser

4. User selects the appropriate method of identification, e-Bank in this case (TUPAS)

5. VETUMA-service
   • creates the request for TUPAS-service
   • forwards the request through the user's browser to the selected Bank's Service Interface (according TUPAS specs)

6. e-Banking Application performs the user identification through the bank's own User Interface

7. e-Banking Application
   • creates the TUPAS-response
   • forwards the response through the user's browser to the VETUMA-service

8. VETUMA-service
   • creates VETUMA-identification response
   • forwards the response through the user's browser to the service application

9. Service Application ensures validity of the response and goes on with the functionality and interaction with user
Use Case: Flow of the VETUMA signature

1. User wants to sign electronically an application
2. Service application
   - ensures that connection uses SSL/TSL
   - creates the request for VETUMA
   - forwards the request through the user’s browser to the VETUMA-service
3. VETUMA-service
   - ensures validity of the request
   - if ok, opens the VETUMA User Interface to the user’s browser and asks the user to start signature
4. User starts the signature and VETUMA-service sends http-response (using https), which activates the Signature Component of user’s browser
5. The Signature Component of the user’s browser asks user to fill in PIN-code and after that produces the signature
6. The signature is forwarded through the user’s browser to VETUMA-service
7. After receiving the signature, VETUMA-service checks the validity of certificates used in signature utilising the service of PRC
8. VETUMA-service
   - creates VETUMA signature-response (including the signature)
   - forwards the response through the user’s browser to the service application
9. Service Application ensures validity of the response and goes on with the functionality and interaction with user
Thank you

Mira Nivala, Project Manager
Public Management Department
Ministry of Finance
Aleksanterinkatu 36 A
P.O.Box 28
00023 Government, FINLAND

Email: mira.nivala@vm.fi
Gsm: +358 400 902 934